Informationssäkerhetspolicy

Fastställd av Förbundsstyrelsen 2018-03-15

Informationssäkerhetspolicyn är Vårdförbundets styrdokument gällande informationshantering. Informationssäkerhet är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder som vidtas för att skydda information. Dokumentet är del i verksamhetsstyrningen.

(Redigerad 2021-11-26: Byte logga samt namnbyte till Integritetsskyddsmyndigheten)

Bakgrund

Vårdförbundet hanterar stora mängder information i verksamheten. En säker informationshantering är avgörande för att fullgöra uppdraget och för att nå verksamhetsmålen. Informationssäkerhet är den samlade effekten av organisatoriska, administrativa och tekniska åtgärder som vidtas för att skydda information.

Informationssäkerhetspolicyn är Vårdförbundets övergripande styrdokument gällande information. Informationssäkerhetspolicyn kompletteras av Behörighetspolicy, Dokument- och arkivplan med gallringstider samt underliggande riktlinjer och arbetsrutiner där den dagliga praktiska hanteringen beskrivs.

Syfte, omfattning och giltighet

Det övergripande syftet med Vårdförbundets informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för information samtidigt som användare behöver tillgång till information för att kunna utföra sitt uppdrag. Policyn omfattar all information inom verksamheten utan undantag, oavsett om informationen behandlas manuellt eller automatiskt, och oberoende av i vilken form eller var i verksamheten informationen förekommer.

Vårdförbundets informationssäkerhetspolicy gäller medlemmar, förtroendevalda tillika skyddsombud, medarbetare och tredje part som har tillgång till information hos Vårdförbundets.
Förbundsstyrelsen beslutar om uppdatering av policyn.

Definitioner

Med *informationssäkerhet* menas bevarandet av konfidentialitet, dvs. att förhindra obehörigt röjande och obehörig åtkomst till uppgifter. Med *informationssäkerhet* avses systematiken i arbetet för att risken för att uppgifter förstörs, förloras eller förändras oavsiktligt minimeras. I *informationssäkerhet* ingår också arbetet kring informations tillgänglighet, så att rätt information är tillgänglig för rätt person när så är bestämt och inte tillgänglig när det är begränsad tillgång som beslutats.

Med *information* avses all typ av information oavsett behandlingsform eller format.

En *informationsmängd* avser information som är avgränsad för ett visst ändamål.

Skyddsnivå är ett begrepp som finns både i personuppgiftslagen och i dataskyddsdirektivet som ersätter tidigare lagstiftning. Förenklat kan man säga att informationer ges olika skyddsnivå, olika värde, och att åtgärder för att skydda informationen behöver beakta känslighetsgraden för informationen och mängden information. Ett för Vårdförbundet relevant exempel är att information om medlemskap i facklig organisation är känslig personuppgift enligt lagstiftningen. När antalet informationsposter är över 100 000 görs t ex tolkningen att ett dataskyddsombud ska tillsättas för att granska verksamhetens hantering. Om medlemskapet istället gällt den lokala fotbollsklubben hade ett eget dataskyddsombud inte behövts. Det är skyddsnivån på informationen som avgör åtgärdens utformning.

Skyddsåtgärd är det som organisationen gör för att minska risken för att t ex personuppgifter sprids till obehöriga eller till parter som inte har en tillräckligt bra hantering. Ett exempel på en skyddsåtgärd är att Vårdförbundet skriver Personuppgiftbiträdesavtal med leverantörer som får tillgång till medlemmars personuppgifter och avtalar kring vilken typ av behandling som får göras och när uppgifterna sen ska rensas. T ex får kontaktinformation till medlemmar inte säljas vidare av våra underleverantörer. Exempel på annan skyddsåtgärd är att begränsa tillgången till de låsta förråd där arkiverade medlemsärenden finns.

Skyddsåtgärder relaterar till informationens skyddsnivå. Man ska särskilt ta hänsyn till vilket slags uppgifter det är fråga om, ändamålet med behandlingen, hur länge behandlingen ska pågå, varifrån uppgifterna ursprungligen kommer, var uppgifterna slutligen kommer att hamna och vilka dataskyddsregler som gäller.

Med *informationsincidentrapport* och *personuppgiftsincident* avses den rapportering som Vårdförbundet är skyldig att göra till Integritetsskyddsmyndigheten (IMY) om information t ex tappas bort eller lämnas ut till obehöriga. Anmälan syftar till att göra det möjligt för Integritetsskyddsmyndigheten att se och bevaka vilka åtgärder som ska vidtas för att motverka negativa effekter av det inträffade.

Ansvar

Förbundsstyrelsen är ytterst ansvarig för informationssäkerheten inom Vårdförbundet. Kanslichef är ansvarig för att organisera arbetet kring informationssäkerhet och för övergripande säkerhetsfrågor av styrande karaktär. Ansvaret omfattar att säkerställa att det finns ekonomiska och personella resurser med rätt kompetens för informationssäkerhetsarbetet.

Alla som hanterar och ges tillgång till Vårdförbundets information i någon form har ett ansvar för att upprätthålla informationssäkerheten och ska följa beslutade och gällande policy, riktlinjer och rutiner. Förtroendevalda, ledare och chefer på alla nivåer har ett särskilt ansvar att kommunicera kring och verka för en god informationssäkerhet. Systemägare ansvarar för informationssäkerheten inom respektive IT-system. Systemförvaltare ansvarar för användning och behörighetsadministration i IT-system.

Informationssäkerhetsarbetet

Vårdförbundets informationssäkerhetsarbete ska bedrivas på ett systematiskt och riskorienterat sätt med hänsyn till tillgängliga resurser. Informationssäkerhetsarbetet utgår från Vårdförbundets uppdrag och den typ av information som följer med verksamheten. Det handlar om att uppfylla verksamhetsbehovet av tillgång till information och samtidigt skydda information.

Medlemmar, förtroendevalda tillika skyddsombud, medarbetare och i vissa fall tredje part ska ha tillgång till den information som behövs för att utföra uppdraget utifrån definierat uppdrag. Informationstillgång och informationsbegränsning ska vara spårbar och utformad på så sätt att det går att säkerställa att information med hög känslighet hanteras på ett korrekt sätt.

- ✓ Informationssäkerheten omfattar all information hos Vårdförbundet. Exempel på information är medlemsinträdesblanketter i pappersformat, listor med medlems personuppgifter och lönenivå, bokföringsmaterial både i formatet pappersfaktura och i formatet digitala registerposter i bokföringsprogrammet.

- ✓ Informationssäkerhetsarbetet utgår från regelbundna riskanalyser som syftar till att säkerställa rätt skyddsnivå för informationen, samt motivera investeringar eller utbildningsinsatser för att uppnå:

  • *Sekretess*, dvs. förhindra eller försvåra för obehöriga att få tillgång till information
  • *Riktighet*, dvs. säkerställa att den information som skapas, sparas och bearbetas är korrekt, aktuell och fullständig
  • *Tillgänglighet*, dvs. bidra till att information är åtkomlig vid behov
  • *Bevarande*, dvs. säkerställa att information inte oavsiktligt ändras eller förloras
  • *Spårbarhet*, dvs. säkerställa ursprunget av varje åtkomst och behandling

  För vart och ett av områdena sekretess, riktighet, tillgänglighet, bevarande och spårbarhet ska organisatoriska, administrativa och tekniska skyddsåtgärder vidtas och dokumenteras på ett sådant sätt att det går att kontrollera att en tillfredsställande skyddsnivå uppnåtts.

- ✓ All information ska klassificeras med en säkerhetsnivå avseende grad av känslighet och informationsmängd. Då kan informationshanteringen organiseras och genomföras utifrån risk. Exempel på åtgärder som påverkas av informationsklassningen är t ex när pseudonymisering ska göras, vilken information som ska krypteras och inte och var lagring av information får ske.

- ✓ En kontinuitetsplan ska finnas för IT-driften, bland annat för att säkerställa förmågan att återställa tillgängligheten till information i rimlig tid vid en fysisk eller teknisk incident.

- ✓ Systemägare ska göra regelbundna säkerhetsbedömningar ska för de IT-system de ansvarar för. Dataskyddsombudet (DSO) ansvarar för att följa upp att så sker och för att resultatet av granskningen rapporteras årligen till förbundsstyrelsen.

- ✓ Samtliga användare, förtroendevalda, medarbetare och tredje parter med informationstillgång ska vara uppmärksamma på och rapportera händelser som kan påverka informationssäkerheten. Rutiner ska finnas för att Vårdförbundet ska kunna fullgöra sin informationsincidentrapportering till tillsynsmyndighet och registrerade inom 72 timmar.

- ✓ Avvikelser och incidenter ska systematiskt dokumenteras och följas upp, så att erfarenheter från dessa kan tas till vara som en del av det kontinuerliga förbättringsarbetet. Allvarligare personuppgiftsincidenter ska rapporteras till DSO och förbundsstyrelsen.